Cybersecurity @INL

Protecting the digital devices that we love to use takes the talents of many people. At Idaho National Laboratory, people with all kinds of backgrounds help protect the nation's industrial control systems from failure. Industrial control systems run important systems like the electric power grid, telecommunication technology, and even transportation hubs like airports or train stations.

Our employees work in teams to study complex machines, electronic circuitry, and computer code. We hire plenty of engineers, computer scientists, and power grid specialists – but we also hire threat intelligence specialists, linguists, and human factors experts. All these skills are necessary when it comes to protecting computer-based equipment that is bought, sold, and used around the world.

Our cybersecurity experts are sometimes referred to as hackers. But not all hackers are bad, despite what you may have seen in the movies. Sometimes the best way to fix a machine is to reverse engineer it – or break it – and put it back together again with more knowledge of how it operates and how it can be better protected.

We work in teams to outsmart the bad hackers.

Our employees are often asked to think how a bad person would try to destroy a piece of important equipment. By channeling an adversarial mindset, our employees can often design engineering fixes to keep the lights on, communication flowing, and traffic moving.

HACKER HATS

In the cybersecurity world, hackers often use pseudonyms – or screen names – to protect their real identity from being disclosed online. But no matter their code name, hackers fall into several different categories.

Black Hats

Black Hats are the type of hacker popular media tends to focus on. They fit the widely held stereotype that hackers are criminals performing illegal activities for personal gain and attacking others. In the real world, black hats are computer criminals.

White Hats

White Hats are the opposite of the black hat hackers. They're the ethical hackers, experts in compromising computer security systems who use their abilities for good, ethical, and legal purposes rather than bad, unethical, and criminal purposes. All of the hackers at INL are white hats.

Gray Hats

Gray Hats fall somewhere between a black hat and a white hat. A gray hat doesn't work for their own personal gain or to cause carnage, but they may technically commit crimes and do arguably unethical things.

INL Idaho National Laboratory

INL STEM AMBASSADORS

STEM.INL.GOV

Red Team/Cell

Red Team/Cell is a group of ethical hackers that attack an organization's digital infrastructure to independently verify how well an organization would fare in the face of a real attack. Red teams are often third-party contractors. At INL, we train people to defend their computer systems from a red team assault.

Blue Team/Cell

Blue Team/Cell is a group of cybersecurity defenders. Blue teams have two major areas of operations. They continually attempt to harden security around and within the company's data systems and networks, and they act as an active part of the defensive systems during a real attack. Blue teams generally work in a company's information technology department. Some of the cybersecurity researchers at INL are blue teamers who work to protect our network. Many companies perform regular exercises under which both red and blue teams are utilized.

HACKING HISTORY

A lot of people think cybersecurity is a new, modern phenomenon. But hackable technologies have existed for generations, and there are plenty of examples where vulnerabilities have been discovered and used to disrupt normal services. In many cases, hackers leave clues to their identity by revealing their code name or the name of their hack deep in the computer script. Some of the more famous hacks include names like: ILOVEYOU, WannaCry, and NotPetya.

HACKING TIMELINE

Here are a few notable hacking events.

1903

Marconi Wireless Hack – In 1903, Italian radio pioneer's Guglielmo Marconi attempted to demonstrate secure Morse code communications. But his live demonstration was interrupted by a hacker who balked at Marconi's claim of secure communications.

1966

Driver Aid, Information and Routing System – In 1966, General Motors Corporation developed the DAIR system for its vehicles. This two-way system was designed to communicate emergency information, traffic conditions, and road hazards from vehicles to service stations. It was the legacy version of today's OnSTAR technology. INL researchers have theorized that any vehicle manufactured after 1966 could potentially be affected through cyber means.

2000

Marooch Water Plant – In 2000, workers at a wastewater treatment plant in Queensland, Australia, faced a dirty, stinky mess. A disgruntled resident hacked the plant's computer system and disrupted communication signals between the plant and nearby pumping stations. During a three-month period, the hacker released 265,000 gallons of untreated sewage into nearby waterways and parks.

2013

Target Corporation – In 2013, hackers broke into the digital heating and cooling control system of department store retailer Target Corporation. Once inside, they installed credit-card-stealing software on cash register terminals across the country. For three weeks, the hackers had access to nearly every customer that made a purchase at one of their stores. The hack compromised nearly 70 million customers and 40 million credit and debit card accounts.

2015-16

Ukraine Power Grid – In 2015 and 2016, the electricity in Kiev, Ukraine, went out for more than 300,000 residents. The twin December hacks became the first known cyberattacks to successfully affect the power grid. The 2016 hack has since been named CRASHOVERRIDE and has led to millions of dollars in research to prevent a similar power outage at other locations around the world.